

**CLAIMS**

What is claimed is:

Sw  
AB

- 1 1. A method comprising:  
2 providing a partition on a storage device of a computer system, wherein  
3 said partition is normally invisible to an operating system of the computer system  
4 unless the partition is unlocked; and  
5 unlocking the partition in response to an unlock request received from a  
6 software task having knowledge about a proper handshake to unlock the  
7 partition, wherein the partition is visible to the operating system when it is  
8 unlocked.
- 1 2. The method of claim 1, wherein the storage device is a hard disk drive  
2 having a disk controller.
- 1 3. The method of claim 1, wherein the unlocking of the partition is initiated  
2 by establishing a proper unlock handshake between the software task and an  
3 IDE controller for controlling the storage device.
- 1 4. The method of claim 3, wherein the software task requests a master  
2 token from the IDE controller when the computer system is first turned on and the  
3 unlock handshake between the software task and the IDE controller is  
4 established by passing the master token back to the IDE controller as a  
5 parameter.
- 1 5. The method of claim 2, wherein the software task requests a master  
2 token from the disk controller when the computer system is first turned on, said  
3 master token is used by the software task to initiate the proper handshake to  
4 unlock the partition.
- 1 6. The method of claim 1, further comprising preventing an access to the  
2 partition when the partition is unlocked unless the access is requested by a  
3 software having knowledge about a proper access handshake for accessing the  
4 partition.

storing the master token in a secure storage location;  
retrieving the master token from the secure storage location when an access to a secure-private partition is needed; and  
passing the master token as a parameter to the IDE controller.

1 13. The machine-readable medium of claim 10, wherein the operations  
2 further comprise requesting an access to the secure-private partition in response  
3 to an access request received from the software.

1 14. The machine-readable medium of claim 13, wherein the requesting of  
2 the access to the secure partition further comprises:

3 receiving a usage token; and  
4 passing the usage token to the IDE controller to gain an access to the  
5 secure partition.

AB  
1 15. The machine-readable medium of claim 10, wherein the request from  
2 the software to access the secure-private partition is received by a privacy  
3 gatekeeper which prescreens the request to determine if the software has an  
4 authorization to access the secure-private partition.

1 16. A system comprising:

2 a storage device having a storage controller, said storage device having at  
3 least one secure-private partition, wherein said secure-private partition is  
4 selectively in one of locked and unlocked modes, wherein said secure-private  
5 partition is invisible to an operating system when it is locked and the secure-  
6 private partition is visible to the operating system when it is unlocked;

7 an IDE controller operatively coupled to the storage controller; and  
8 a security/privacy software task operatively coupled to the IDE controller,  
9 wherein said IDE controller initiates an unlock request to unlock the secure-  
10 private partition in response to a valid unlock handshake established between the  
11 IDE controller and the security/privacy software task and said IDE controller  
12 initiates a lock request to lock the secure-private partition in response to a valid  
13 lock handshake established between the IDE controller and the security/privacy  
14 software task.

1 17. The system of claim 16, wherein the security/privacy software task  
2 requests a master token from the IDE controller when the system is turned on  
3 and sends the master token to the IDE controller as a parameter when making a  
4 request to the IDE controller to unlock the secure-private partition.

1 18. The system of claim 16, further comprising a requesting software and  
2 a privacy gatekeeper which acts as a gatekeeper to the security/privacy software  
3 task, wherein when the requesting software makes a request to access the  
4 secure-private partition, the privacy gatekeeper prescreens the request to  
5 determine if the requesting software has an authorization to access the secure-  
6 private partition.

1 19. The system of claim 18, wherein the IDE controller allows an access  
2 to said at least one secure-private partition only when a valid access handshake  
3 is established between the requesting software and the IDE controller.

1 20. The system of claim 19, wherein the IDE controller generates and  
2 return a usage token to the requesting software once the secure-private partition  
3 is unlocked, wherein the access handshake is established between the IDE  
4 controller and the requesting software when the IDE controller validates the  
5 usage token passed back by the requesting software.